

Table of Contents

PART I THE BASICS

| | |
|--|-----------|
| Chapter 1 Security Foundations | 3 |
| The Basics | 4 |
| <i>Threats and Risk</i> | 4 |
| <i>Understanding the Technology</i> | 6 |
| <i>The Tools</i> | 7 |
| Darwin | 8 |
| The Command Line | 9 |
| UNIX Security | 10 |
| <i>Users and Groups</i> | 10 |
| Introducing NetInfo | 16 |
| NetInfo Security | 17 |
| Summary | 20 |
| Chapter 2 Installation | 21 |
| To BSD or Not to BSD | 22 |
| Filesystems—HFS+ Versus UFS | 25 |
| <i>A Tale of Two Filesystems</i> | 25 |
| <i>Security Considerations</i> | 25 |
| Mac OS X Install Step-by-Step | 28 |
| <i>Physical Setup</i> | 28 |
| <i>Beginning the Installation</i> | 28 |
| <i>Choosing and Partitioning the Disk</i> | 29 |
| <i>Customizing the Install</i> | 32 |
| <i>The Setup Assistant (Mac OS X Client)</i> | 34 |
| <i>The Setup Assistant (Mac OS X Server)</i> | 36 |
| <i>Developer Tools</i> | 41 |
| Summary | 41 |

PART II SYSTEM SECURITY

| | |
|---|-----------|
| Chapter 3 Mac OS X Client General Security Practices | 45 |
| Concerns About Physical Access | 46 |
| <i>Doors, Locks, and Guards</i> | 47 |
| <i>Open Firmware Password</i> | 47 |
| <i>Login Window</i> | 50 |
| <i>Screen Locking</i> | 52 |
| <i>System Preferences Locking</i> | 53 |
| Dual Booting and the Classic Environment | 54 |
| <i>Classic and OS 9</i> | 54 |
| <i>Dual Booting Dangers</i> | 55 |

| | |
|--|-----------|
| Staying Current with OS X | 56 |
| User Accounts and Access Control | 58 |
| Filesystem Encryption | 61 |
| Summary | 64 |
| Chapter 4 What Is This UNIX Thing? | 65 |
| The Command Line Interface | 66 |
| <i>Command Line Access</i> | 66 |
| <i>Command Line Security</i> | 68 |
| Directories, Permissions, and File Ownership | 70 |
| <i>File Security and Permissions</i> | 71 |
| <i>Special File Permissions</i> | 74 |
| <i>How to Modify Permissions and Ownership</i> | 78 |
| <i>Using Get Info to Modify Permissions</i> | 82 |
| Common UNIX Commands | 84 |
| <i>top</i> | 84 |
| <i>ps</i> | 85 |
| <i>kill and killall</i> | 86 |
| <i>last and who</i> | 88 |
| <i>find</i> | 88 |
| <i>netstat</i> | 89 |
| <i>openssl</i> | 90 |
| UNIX Security | 91 |
| <i>SUID and SGID Files</i> | 91 |
| <i>Kernel Security Levels</i> | 92 |
| <i>sudo</i> | 93 |
| Summary | 97 |
| Chapter 5 User Applications | 99 |
| General Application Security Considerations | 100 |
| Keychain | 102 |
| <i>Using the Keychain Access Application</i> | 103 |
| <i>Is the Keychain Safe?</i> | 108 |
| Mail.app Security | 108 |
| <i>Using SSL to Send and Receive Mail</i> | 109 |
| <i>Using SSH to Send and Receive Mail</i> | 111 |
| <i>Keeping Mail Off the Server</i> | 113 |
| <i>Storing Mail on an Encrypted Disk</i> | 114 |
| <i>Using PGP to Encrypt Email</i> | 114 |
| <i>Using GnuPG to Encrypt Email</i> | 118 |
| Web Browser Security Issues | 121 |
| <i>Web Browsing and SSL</i> | 121 |
| <i>Cookie and Cache Management</i> | 122 |
| Summary | 127 |

PART III NETWORK SECURITY

| | |
|--|------------|
| Chapter 6 Internet Services | 131 |
| Web Services | 132 |
| <i>Mac OS X Configuration Oddities</i> | 133 |
| <i>General Security Considerations</i> | 136 |
| <i>Running Apache on a Non-privileged Port</i> | 140 |
| <i>Putting Apache in a Jail</i> | 146 |
| <i>Configuring Authenticated Access</i> | 154 |
| SSL | 161 |
| Email Services | 170 |
| <i>Sendmail</i> | 170 |
| <i>MailService</i> | 171 |
| FTP | 177 |
| Remote Login (SSH) | 178 |
| <i>Security Considerations</i> | 179 |
| <i>SSH Tunnels</i> | 181 |
| Remote Apple Events | 182 |
| <i>Security Considerations</i> | 182 |
| Xinetd | 183 |
| <i>Configuring xinetd in Mac OS X</i> | 183 |
| Summary | 190 |
| Chapter 7 File Sharing | 191 |
| WebDAV Services | 192 |
| <i>Security Considerations</i> | 193 |
| <i>Setting Up Secure WebDAV Services on Mac OS X</i> | 194 |
| <i>Additional WebDAV Options</i> | 199 |
| Apple File Services | 200 |
| <i>AFS Security Model</i> | 200 |
| <i>Configuring AFS Via Server Settings</i> | 201 |
| <i>Configuring AFS Via Workgroup Manager</i> | 202 |
| SMB File Services | 203 |
| <i>SMB Security Models</i> | 203 |
| <i>Configuration Through Server Settings</i> | 204 |
| <i>Configuration Through Workgroup Manager</i> | 205 |
| <i>Configuration Through Terminal</i> | 207 |
| <i>Logging</i> | 208 |
| Network File System | 209 |
| <i>NFS Structure</i> | 210 |
| <i>Configuring NFS Through Server Settings</i> | 210 |
| <i>Configuring NFS Through Workgroup Manager</i> | 210 |
| <i>Configuring NFS Through Terminal</i> | 211 |
| <i>Re-Exporting Via AFS</i> | 212 |
| Personal File Sharing | 212 |
| Making Secure AFS Connections | 214 |
| Summary | 216 |

| | |
|---|------------|
| Chapter 8 Network Services | 217 |
| Firewalling | 218 |
| <i>Using Built-in Tools</i> | 219 |
| <i>Manually Configuring the Firewall</i> | 226 |
| <i>Alternatives to Apple</i> | 228 |
| VPN | 228 |
| IPSec | 228 |
| PPTP | 231 |
| AirPort Security | 234 |
| <i>Configuring WEP</i> | 234 |
| <i>Using LEAP</i> | 236 |
| <i>Static ARP</i> | 236 |
| <i>Software Base Station</i> | 238 |
| Antivirus Protection | 239 |
| <i>Common Sense</i> | 239 |
| <i>Antivirus Software</i> | 241 |
| Summary | 242 |
| | |
| PART IV ENTERPRISE SECURITY | |
| <hr/> | |
| Chapter 9 Enterprise Host Configuration | 245 |
| Login Window | 246 |
| <i>Changing the Login Window Graphic</i> | 246 |
| <i>Adding a Login Banner</i> | 247 |
| <i>Using Kerberos Authentication</i> | 248 |
| Kerberos | 248 |
| <i>Integrating Mac OS X Clients into a Kerberos Environment</i> | 249 |
| <i>Using Kerberized Services on Mac OS X Server</i> | 250 |
| Rendezvous | 253 |
| <i>Rendezvous Security</i> | 254 |
| Summary | 255 |
| Chapter 10 Directory Services | 257 |
| Yet Another “The Basics” | 258 |
| NetInfo | 259 |
| <i>Authentication</i> | 263 |
| <i>Authorization</i> | 263 |
| <i>Data Privacy</i> | 266 |
| Open Directory | 266 |
| <i>Connecting Mac OS X to an Open Directory Server</i> | 268 |
| <i>Authentication</i> | 270 |
| <i>Authorization</i> | 270 |
| <i>Data Privacy</i> | 272 |

| | |
|--------------------------------|-----|
| More Fun with Directory Access | 274 |
| <i>AppleTalk</i> | 274 |
| <i>BSD Configuration Files</i> | 274 |
| <i>LDAPv2</i> | 275 |
| <i>LDAPv3</i> | 276 |
| <i>NetInfo</i> | 276 |
| <i>Rendezvous</i> | 276 |
| <i>SLP</i> | 276 |
| <i>SMB</i> | 276 |
| Summary | 277 |

PART V AUDITING AND FORENSICS

| | |
|--|------------|
| Chapter 11 Auditing | 281 |
| The Importance of Logging | 282 |
| General Considerations | 282 |
| <i>The Importance of Time</i> | 282 |
| <i>Permissions and Access</i> | 284 |
| <i>Log Rotation</i> | 284 |
| <i>Log Archives and Secure Storage</i> | 285 |
| Logging Options and Configuration | 285 |
| <i>Syslog</i> | 286 |
| <i>Logging Network Services</i> | 289 |
| <i>CrashReporter</i> | 292 |
| Monitoring Logs | 295 |
| <i>The Basics</i> | 295 |
| <i>Automated Monitoring and Notification with swatch</i> | 297 |
| Log Location Reference | 301 |
| Summary | 303 |
| Chapter 12 Forensics | 305 |
| An Overview of Computer Forensics | 306 |
| <i>Acquisition</i> | 306 |
| <i>Analysis</i> | 308 |
| Osiris | 309 |
| <i>General Security Considerations</i> | 310 |
| <i>Installing Osiris</i> | 312 |
| <i>Configuring and Automating Osiris</i> | 313 |
| <i>Using Osiris to Monitor SUID Files</i> | 316 |
| <i>Using scale</i> | 316 |
| Forensic Analysis with TASK | 318 |
| <i>Overview of TASK</i> | 318 |
| <i>Getting the Data</i> | 319 |
| <i>Analysis with TASK</i> | 321 |
| Summary | 325 |

| | |
|--|------------|
| Chapter 13 Incident Response | 327 |
| What Does Incident Response Mean to You? | 328 |
| Incident Response Life Cycle | 329 |
| <i>Preparation</i> | 330 |
| <i>Detection and Assessment</i> | 336 |
| <i>Response</i> | 337 |
| <i>Postmortem</i> | 339 |
| Summary | 340 |

PART VI APPENDIXES

| | |
|--|------------|
| A SUID and SGID Files | 343 |
| SUID Files | 348 |
| SGID Files | 349 |
| B Common Data Security Architecture | 351 |
| Benefits of the CDSA | 352 |
| CDSA Structural Overview | 352 |
| <i>Add-in Modules</i> | 353 |
| <i>Common Security Services Manager (CSSM)</i> | 354 |
| <i>Security Services</i> | 355 |
| <i>Apple's CDSA Security Services</i> | 356 |
| <i>A Note to Developers</i> | 359 |
| C Further Reading | 361 |
| Chapter 1—Security Foundations | 362 |
| Chapter 2—Installation | 362 |
| Chapter 3—OS X Client General Security Practices | 363 |
| Chapter 4—What Is This UNIX Thing? | 364 |
| Chapter 5—User Applications | 364 |
| Chapter 6—Internet Services | 365 |
| Chapter 7—File Sharing | 366 |
| Chapter 8—Network Services | 366 |
| Chapter 9—Enterprise Host Configuration | 367 |
| Chapter 10—Directory Services | 367 |
| Chapter 11—Auditing | 368 |
| Chapter 12—Forensics | 368 |
| Chapter 13—Incident Response | 369 |
| Index | 371 |